

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-108778

(43)Date of publication of application : 12.04.2002

(51)Int.Cl. G06F 13/00  
G06F 11/00  
H04L 12/54  
H04L 12/58

(21)Application number : 2000-293482

(71)Applicant : JAPAN BUSINESS COMPUTER CO  
LTD

(22)Date of filing : 27.09.2000

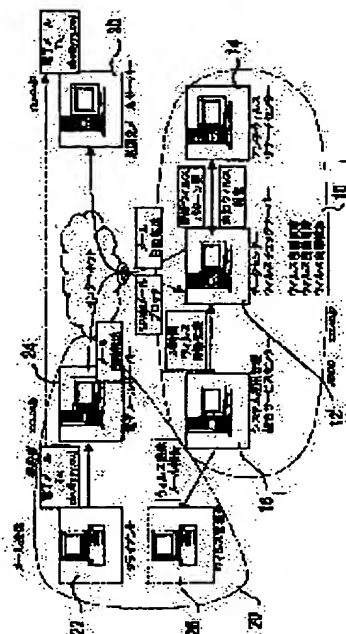
(72)Inventor : UCHIUMI TOSHIHIRO

## (54) VIRUS CHECKING SERVER AND VIRUS CHECKING METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To take countermeasures against a virus of an electronic mail without the need of individual facilities.

**SOLUTION:** An electronic mail transmitted from the client terminal 22 of a client network 20 to an electronic mail server 24 is transferred to the virus checking server 12 of a virus checking system 10 from the electronic mail server 24. The virus checking server 12 receives and preserves the electronic mail and transfers the electronic mail which is virus-checked and to which necessary processing is applied for removing the virus to a transmission destination/transmission source electronic mail server 30 being a destination.



## LEGAL STATUS

[Date of request for examination] 25.09.2001

[Date of sending the examiner's decision of rejection] 18.04.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-108778

(P2002-108778A)

(43)公開日 平成14年4月12日(2002.4.12)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-リ-ト*(参考)
G 0 6 F 13/00	6 1 0	G 0 6 F 13/00	6 1 0 Q 5 B 0 7 6
	3 5 1		3 5 1 Z 5 B 0 8 9
11/00		9/06	6 6 0 N 5 K 0 3 0
H 0 4 L 12/54		H 0 4 L 11/20	1 0 1 B
12/58			

審査請求 有 請求項の数12 O L (全 13 頁)

(21)出願番号 特願2000-293482(P2000-293482)

(22)出願日 平成12年9月27日(2000.9.27)

(71)出願人 591082225

日本ビジネスコンピューター株式会社

東京都大田区蒲田五丁目37番1号 ニッセ  
イアロマスクエア

(72)発明者 内海 俊洋

東京都大田区蒲田5-37-1 ニッセイア  
ロマスクエア15F 日本ビジネスコンピ  
ューター株式会社内

(74)代理人 100086209

弁理士 網野 友康 (外2名)

Fターム(参考) 5B076 FD08 FD09

5B089 GA11 GA21 JA31 KA17 KB13

KC52 KC54 LA08

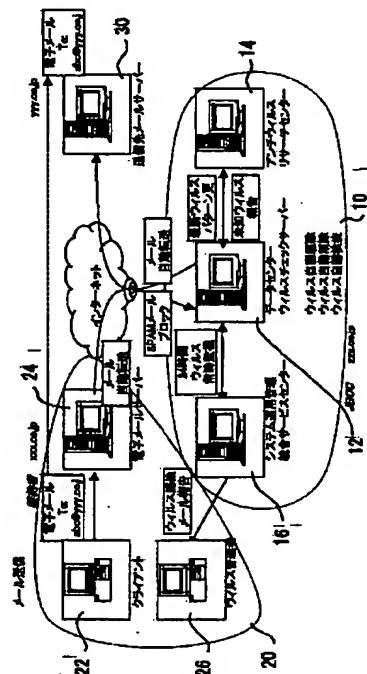
5K030 GA15 HA06 HC01

(54)【発明の名称】 ウイルスチェックサーバ及びウイルスチェック方法

(57)【要約】

【課題】 個別に設備を要することなく電子メールのウイルス対策を実現する。

【解決手段】 クライアントネットワーク20のクライアント端末22から電子メールサーバ24に送信された電子メールは、電子メールサーバ24からウイルスチェックシステム10のウイルスチェックサーバ12に転送される。ウイルスチェックサーバ12は電子メールを受信して保管し、ウイルスチェック及び必要なウイルス駆除を経た電子メールを、宛先となる送信先/送信元電子メールサーバ30に転送する。



## 【特許請求の範囲】

【請求項 1】 一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールを受信して保管する電子メール保管手段と、

前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック手段と、

前記ウイルスチェック手段によりウイルスチェック済みの前記電子メールを前記他の電子メールサーバに転送する電子メール転送手段とを含むことを特徴とするウイルスチェックサーバ。

【請求項 2】 前記一つの電子メールサーバは、クライアント側電子メールサーバであり、

前記電子メール保管手段は前記クライアント側電子メールサーバから送信される前記電子メールの全てを受信して保管する請求項 1 に記載のウイルスチェックサーバ。

【請求項 3】 前記他の電子メールサーバのうちの 하나는クライアント側電子メールサーバであり、

前記電子メール保管手段は前記クライアント側電子メールサーバに送信される前記電子メールの全てを受信して保管する請求項 1 に記載のウイルスチェックサーバ。

【請求項 4】 前記一つの電子メールサーバ及び前記他の電子メールサーバのうちの 하나는同じクライアント側電子メールサーバであり、

前記電子メール保管手段は前記クライアント側電子メールサーバに送信され、及び前記クライアント側電子メールサーバから送信される前記電子メールの全てを受信して保管する請求項 1 に記載のウイルスチェックサーバ。

【請求項 5】 前記電子メール保管手段が前記電子メールを保管する前に、前記電子メールの SPAM チェックを行う SPAM チェック手段をさらに含む請求項 1 ないし 4 に記載のウイルスチェックサーバ。

【請求項 6】 一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールを受信して電子メール保管手段に保管する電子メール保管過程と、

前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック過程と、

前記ウイルスチェック過程においてウイルスチェック済みの前記電子メールを前記他の電子メールサーバに転送する電子メール転送過程とを含むことを特徴とするウイルスチェック方法。

【請求項 7】 前記一つの電子メールサーバ及び前記他の電子メールサーバのうちの 하나는同じクライアント側電子メールサーバであり、

前記電子メール保管過程において、前記クライアント側電子メールサーバに送信され、及び前記クライアント側電子メールサーバから送信される前記電子メールの全て

が前記電子メール保管手段に受信されて保管される請求項 6 に記載のウイルスチェック方法。

【請求項 8】 前記電子メール保管過程において、前記クライアント側電子メールサーバから送信される送信電子メールは、前記クライアント側電子メールサーバの SMTP サーバのリレー先として前記電子メール保管手段を指定することにより、前記送信電子メールの全てが前記電子メール保管手段に受信されて保管され、かつ前記クライアント側電子メールサーバに受信される受信電子メールは、DNS サーバに記述された前記クライアント側電子メールサーバについての MX レコードを前記電子メール保管手段が宛先になるように書き換えることにより、前記受信電子メールの全てが前記電子メール保管手段に受信されて保管される請求項 7 に記載のウイルスチェック方法。

【請求項 9】 前記電子メール保管過程の前に、前記電子メールの SPAM チェックを行う SPAM チェック過程をさらに含む請求項 6 ないし 8 に記載のウイルスチェック方法。

【請求項 10】 前記ウイルスチェック過程は、前記電子メール保管手段に保管された前記電子メールを読み出してウイルス定義テーブルに予め記憶された既知ウイルスとのマッチングを行うことによりウイルスに感染しているか否かを判定するウイルス感染チェック過程と、

ウイルスに感染していると判定された前記電子メールのウイルス駆除を行うウイルス駆除過程と、

ウイルス駆除に失敗した場合に前記電子メールのウイルス削除を行うウイルス削除過程と、

駆除または削除されたウイルス媒体の検疫を行うウイルス媒体検疫過程とを含む請求項 6 ないし 9 に記載のウイルスチェック方法。

【請求項 11】 前記ウイルス感染チェック過程においてウイルスに感染していると判定された場合に、ウイルスに感染していると判定された前記電子メールを送信した端末またはネットワークに対し報告を行う報告過程を含む請求項 10 に記載のウイルスチェック方法。

【請求項 12】 前記報告を行った前記端末またはネットワークに対し、前記端末またはネットワークからウイルスを駆除するためのウイルス駆除手段を提供し、及び／またはウイルス駆除方法を教示するウイルス駆除支援過程を含む請求項 11 に記載のウイルスチェック方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、主としてインターネットを介して授受される電子メールに含まれるウイルスをチェックするためのウイルスチェックサーバ及びウイルスチェック方法に関し、特に電子メールが宛先に到着する以前にウイルスチェックを行うことのできるウイルスチェックサーバ及びウイルスチェック方法に関する

る。

【0002】

【従来の技術】現在、コンピュータウイルスの感染源の80%は電子メールであるといわれている。周知のように、ウイルスに感染し、発症してしまうとシステムがダウンして復旧までに多大な時間的損失を被ることになるのみならず、顧客リスト等の資産的価値の高い情報が消失するといった経済的な損害を与えることになる。また発症する前にウイルスに感染した電子メールを発信した結果、取引先にウイルスを伝染させることになり、企業としての信用問題に関わることになる。よって電子メール利用者は、ウイルス対策に万全を期さなければならない。

【0003】一般的なウイルス対策として、LANのようなネットワーク全体を防御するためにはゲートウェイ用アンチウイルスサーバが利用されている。端末単位ではアンチウイルスソフトをインストールすることが行われている。しかしながらアンチウイルスサーバの導入及び運用管理には多大な人手と時間と費用がかかる。またウイルスに感染しているか否かは既知ウイルスとのパターンマッチングを行うことにより判定するのが一般的であり、このためアンチウイルスサーバやアンチウイルスソフトには頻繁に既知ウイルスのデータをアップデートしなければならない。これを怠ったために新たに発見されたウイルスに対応できず、高価なハードやソフトが何の役にも立たないことがあった。

【0004】

【発明が解決しようとする課題】よって本発明の目的は、最新の既知ウイルスのデータを用いて、安価かつ簡便に電子メールを通じたウイルス感染からシステムを防御できるウイルスチェックサーバ及びウイルスチェック方法を提供することにある。

【0005】

【課題を解決するための手段】上記目的を達成するために本発明は、一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールを受信して保管する電子メール保管手段と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック手段と、前記ウイルスチェック手段によりウイルスチェック済みの前記電子メールを前記他の電子メールサーバに転送する電子メール転送手段とを含んでウイルスチェックサーバを構成した。

【0006】本発明に係るウイルスチェックサーバにおいては、電子メールサーバから送信された電子メールは直接宛先の電子メールサーバに到着せず、いったん電子メール保管手段に保管される。電子メール保管手段に保管された電子メールは、ウイルスチェック手段により読み出されてウイルスチェックを受ける。電子メール転送手段は、ウイルスチェック手段によりウイルスチェッ

ク済みの電子メールを転送し、電子メールが宛先の電子メールサーバに到着する。

【0007】従って本発明に係るウイルスチェックサーバによると、電子メールサーバ間に一つのウイルスチェックサーバを介することにより複数の電子メールサーバに入出力される電子メールのウイルスチェックを行うことができる。従って電子メールサーバが含まれるネットワークや端末ごとにウイルス対策のためのハードやソフトを用意する場合に比較して安価にウイルスチェックを行うことができ、また一箇所で最新のウイルス情報を収集すれば足りるのでチェック漏れも最小限に抑えることが可能である。

【0008】ウイルスチェックサーバによるウイルスチェックは、特定の電子メールサーバに関わる電子メールのみをクライアントとして行うことができる。例えば一つの電子メールサーバは、クライアント側電子メールサーバであり、電子メール保管手段はクライアント側電子メールサーバから送信される電子メールの全てを受信して保管するようにする。また、他の電子メールサーバのうちの一つはクライアント側電子メールサーバであり、電子メール保管手段はクライアント側電子メールサーバに送信される電子メールの全てを受信して保管する。さらに、一つの電子メールサーバ及び他の電子メールサーバのうちの一つは同じクライアント側電子メールサーバであり、電子メール保管手段はクライアント側電子メールサーバに送信され、及びクライアント側電子メールサーバから送信される電子メールの全てを受信して保管する。

【0009】これらの場合、クライアント側電子メールサーバと電子メール保管手段とはインターネット、専用線、フレームリレーなどを通じて電子メールの送受信が可能に接続される。

【0010】さらにまた、電子メール保管手段が電子メールを保管する前に、電子メールのSPAMチェックを行うSPAMチェック手段をさらに含むようにしてもよい。SPAMチェックは、例えばクライアント側電子メールサーバ宛に送信されてきた受信電子メールについては電子メールアドレスのドメイン名をチェックし、クライアント側電子メールサーバから送信された送信電子メールについてはクライアント側電子メールサーバのIPアドレスをチェックすることにより行われる。

【0011】また本発明は、一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールを受信して電子メール保管手段に保管する電子メール保管過程と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック過程と、前記ウイルスチェック過程においてウイルスチェック済みの前記電子メールを前記他の電子メールサーバに転送する電子メール転送過程とを含んでウイルスチェック方法を構成

した。

【0012】本発明に係るウイルスチェック方法においては、電子メールサーバから送信された電子メールは直接宛先の電子メールサーバに到着せず、いったん電子メール保管手段に保管される。電子メール保管手段に保管された電子メールは読み出されてウイルスチェックを受け、ウイルスチェック済みの電子メールが転送され、宛先の電子メールサーバに到着する。

【0013】従って本発明に係るウイルスチェック方法によると、電子メールサーバ間においてウイルスチェックするようにしたので複数の電子メールサーバに入出力される電子メールのウイルスチェックを一箇所で行うことができる。従って電子メールサーバが含まれるネットワークや端末ごとにウイルス対策のためのハードやソフトを用意する場合に比較して安価にウイルスチェックを行うことができ、また一箇所で最新のウイルス情報を収集すれば足りるのでチェック漏れも最小限に抑えることが可能である。好ましくは複数のクライアントとウイルスチェックサーバの管理者とが提携ないし契約を行い、各クライアントがウイルスチェックサーバの維持管理の費用を負担する運用形態が採られよう。

【0014】ウイルスチェックは、特定の電子メールサーバに関わる電子メールのみをクライアントとして行うことができる。例えば一つの電子メールサーバ及び他の電子メールサーバのうちの一つは同じクライアント側電子メールサーバであり、電子メール保管過程において、クライアント側電子メールサーバに送信され、及びクライアント側電子メールサーバから送信される電子メールの全てが電子メール保管手段に受信されて保管されるようにすることができる。

【0015】このためには、電子メール保管過程において、クライアント側電子メールサーバから送信される送信電子メールは、クライアント側電子メールサーバのSMTPサーバのリレー先として電子メール保管手段を指定することにより、送信電子メールの全てが電子メール保管手段に受信されて保管され、かつクライアント側電子メールサーバに受信される受信電子メールは、DNSサーバに記述されたクライアント側電子メールサーバについてのMXレコードを電子メール保管手段が宛先になるように書き換えることにより、受信電子メールの全てが電子メール保管手段に受信されて保管される構成とすることができる。電子メール保管過程の前に、電子メールのSPAMチェックを行うSPAMチェック過程をさらに含むようにしてもよい。

【0016】例えばウイルスチェック過程は、電子メール保管手段に保管された電子メールを読み出してウイルス定義テーブルに予め記憶された既知ウイルスとのマッチングを行うことによりウイルスに感染しているか否かを判定するウイルス感染チェック過程と、ウイルスに感染していると判定された電子メールのウイルス駆除を行

うウイルス駆除過程と、ウイルス駆除に失敗した場合に電子メールのウイルス削除を行うウイルス削除過程と、駆除または削除されたウイルス媒体の検疫を行うウイルス媒体検疫過程とを含んで構成することができる。

【0017】ここで「ウイルス駆除」とは、電子メールまたは電子メールの添付ファイルに感染しているウイルスのみの部分を削除することをいう。「ウイルス削除」とはウイルスに感染している添付ファイルをファイルごと削除することをいう。ウイルス駆除を行った場合には電子メールには添付ファイルは残るが、ウイルス削除をした場合には添付ファイルは残らず、電子メール本文のみになる。またウイルス感染チェックにおいてはパターンマッチングの他、ミューテーション型ウイルスを発見するためのソフトマウス法、未知ウイルスの発見のためのチェックサム方式やトラップ方式などが併用されていてもよい。ウイルス媒体検疫過程においては、ウイルス媒体の保管・集中管理が行われ、さらに検疫されたウイルス媒体を公共や私設のアンチウイルスリサーチセンターに転送して検査や未知ウイルスに対するワクチンの作成をしてもらうことができる。

【0018】ウイルス感染チェック過程においてウイルスに感染していると判定された場合に、ウイルスに感染していると判定された電子メールを送信した端末またはネットワークに対し報告を行う報告過程を含むことができる。これにより、電子メールを送信した者はシステムにウイルスが感染していることを知って、直ちにワクチンなどを使用して治療を行うことができる。報告は、例えば電子メールにて行う。さらに、報告を行った端末またはネットワークに対し、端末またはネットからウイルスを駆除するためのウイルス駆除手段を提供し、及び／またはウイルス駆除方法を教示するウイルス駆除支援過程を含むようにしてもよい。例えば、ウイルスを治療するためのワクチンとその使用方法を電子メールと添付ファイルにより送信する。

【0019】

【発明の実施の形態】以下、本発明に係るウイルスチェックサーバの一つの実施の形態について、添付の図面を参照しつつ説明する。

【0020】図1、2は本発明に係るウイルスチェックサーバの一つの実施の形態の主要な構成を示すブロック図である。

【0021】各図において、ウイルスチェックシステム10は、ウイルスチェックを行うウイルスチェックサーバ12、ウイルスの調査やワクチン作成等を行うアンチウイルスリサーチセンター14及びウイルスチェックサーバ12のチェック状況の監視を行うシステム運用管理統合サービスセンター16からなる。ウイルスチェックシステム10の管理者と契約してウイルスチェックサーバ12を利用するクライアントネットワーク20は、複数のクライアント端末22（1つしか図示していな

い)、電子メールサーバ24及びウイルス管理者端末26を含む。電子メールサーバ24は任意の送信先/送信元電子メールサーバ30との間でインターネットを通じて電子メールの送受信を行う。クライアントネットワーク20は一つしか示していないが、ウイルスチェックシステム10の管理者は複数のクライアントと契約してウイルスチェックサービスを提供することができるというまでもない。

【0022】ウイルスチェックサーバ12は、アンチウイルスリサーチセンター14から最新ウイルスパターン10の供給を受け、パターンファイルの更新を随時行っている。アンチウイルスリサーチセンター14は、ウイルスチェックサーバ12が発見した未知ウイルスについて報告を受け、最新ウイルスパターンやワクチンの作成を行う。システム運用管理統合サービスセンター16は、ウイルスチェックサーバ12のチェック状況を24時間体制で常時監視しており、ウイルスが発見された場合にはウイルス管理者端末26に対して直ちにウイルス感染の事実を電子メールにより報告する。ウイルスチェックサーバ12、アンチウイルスリサーチセンター14及びシステム運用管理統合サービスセンター16は、物理的に一台のコンピュータ内にモジュールとして構成することもできるが、通常はそれぞれ独立のコンピュータであって、専用線やインターネットを介して相互に接続されている。本実施の形態においては、アンチウイルスリサーチセンター14は、公的または私設のウイルス対策のための機関に設置されたコンピュータである。

【0023】図1に示すように、クライアント端末22からabc@yyy.co.jpのメールアドレス宛に電子メールが発信されると、電子メールサーバ24はインターネットを介してウイルスチェックサーバ12に電子メールの転送を行う。ウイルスチェックサーバ12は電子メールのウイルスチェックを行い、ウイルスが含まれていた場合には自動駆除や自動削除を施してから、送信先/送信元電子メールサーバ30へ自動転送する。よって破線で示す電子メールは、仮想的には、電子メールサーバ24から送信先/送信元電子メールサーバ30に直接送信されたように見える。同様に図2のように送信先/送信元電子メールサーバ30からabc@xxx.co.jp宛に発信された電子メールは、ウイルスチェックサーバ12を経由して電子メールサーバ24により受信される。

【0024】図3は、クライアント端末22から電子メールを送信する際の各部材の機能を表すブロック図であり、図4はクライアント端末22が電子メールを受信する際の各部材の機能を表すブロック図である。

【0025】図3において、電子メールサーバ24はクライアント端末22から発信された電子メールがウイルスチェックサーバ12に自動転送されるように設定されている。すなわち、クライアント端末22が電子メールサーバ24に電子メールを送信すると、SMTPサーバ

のリレー先にはウイルスチェックサーバ12のアドレスzzz@co.jpが指定されているので、クライアント端末22からの電子メールは全てウイルスチェックサーバ12に転送される。

【0026】また図4において、送信先/送信元電子メールサーバ30からクライアント端末22宛に電子メールが発信する際、送信先/送信元電子メールサーバ30は宛先ドメインの電子メールサーバを探すためにDNSサーバ40のMXレコードを参照する。クライアント端末22のMXレコードはウイルスチェックサーバ12のものに変更されているので、クライアント端末22宛の電子メールは全てウイルスチェックサーバ12に送信される。

【0027】ウイルスチェックサーバ12は、SPAMチェック部121と、受信メール保管部122と、ウイルスチェック部123と、ウイルス駆除・削除部124と、ロギング部125と、ウイルス検疫部126と、駆除済メール転送部127と、転送済メール削除部128とを含む。

【0028】図5はクライアント側の電子メールサーバ24から送信先/送信元電子メールサーバ30宛に電子メールが送信された場合のデータの授受及びウイルスチェックサーバ12の各部の機能を説明する図である。

【0029】SPAMチェック部121は、SPAMチェックテーブル1212を備えており、SPAMチェックテーブル1212にはクライアント端末の電子メールアドレスのドメイン名及び電子メールサーバのIPアドレスが各クライアントごとに格納されている。まず、電子メールサーバ24から送信された電子メールについてはIPアドレスがチェックされ、予めSPAMチェックテーブル1212に記憶されていた、例えば192.168.x.x.xxと172.16.x.xx以外のIPアドレス以外の電子メールをSPAMとして認識し、受信を拒絶することにより不正中継リレーなどによるSPAMメールの送信を防止している。また、電子メールサーバ24宛の電子メールについては、予めSPAMチェックテーブル1212に記憶されている以外のドメイン名の電子メールはSPAMと認識し、クライアント端末22にSPAMメールが送られないようにする。

【0030】送信元となる電子メールサーバ24は、クライアント端末22から電子メールを受け取ると、ウイルスチェックサーバ12に対しコネクション接続要求(TCPポート25番)を送信し、ウイルスチェックサーバ12は220 Service readyを返信する。次にウイルスチェックサーバ12はIPアドレスを受信するが、SPAMチェック部121によりSPAMメールと認識されると、電子メールの受け取りを拒絶して、メールセッションを破棄する。

【0031】SPAMチェックをパスした場合には、電子メールサーバ24から電子メールの本文(及び添付フ

ファイル)となるデータがウイルスチェックサーバ12に送信され、受信メール保管部122のキュー1222に記憶される。全てのデータが送信され終わるとコネクションが切断される。

【0032】ウイルスチェック部123においてはキュー1222から読み出したデータとウイルス定義テーブル1232に格納された既知ウイルスのパターンとのマッチングが行われる。もしもウイルスが発見されると、ウイルス駆除・削除部124によるウイルスの駆除または削除が行われる。まず、電子メールの添付ファイルに感染しているウイルスの削除であるウイルス駆除が試みられる。これに失敗した場合、ウイルスに感染した添付ファイルを添付ファイルごと削除するウイルス削除が行われる。これにより、電子メールからウイルスが取り除かれる。駆除または削除されたウイルス媒体はログ部125のログに書き出され、さらにウイルス検疫部126により保管、集中管理される。

【0033】ウイルスチェックをパスした電子メール、及びウイルス駆除または削除の済んだ電子メールは、駆除済メール転送部127のキュー1272に送信されて記憶され、その後宛先となる送信先/送信元電子メールサーバ30にインターネットを介して転送される。転送された電子メールは転送済メール削除部128によりキュー1272から削除される。

【0034】図6及び図7は、図1～5に示したウイルスチェックサーバ12の処理の流れを示すフローチャートである。

【0035】まず、クライアント端末22から電子メールを送信するメール送信の場合の処理の流れを示す図6について説明する。

【0036】クライアントは、従来の電子メール送信手順と同様にして電子メールの発信を行う。すなわち電子メールの宛先のメールアドレスを記入し、クライアント端末22から電子メールサーバ24に電子メールを送信する(ステップS601)。しかし電子メールサーバ24は、SMTPサーバのリレー先が指定されているので、電子メールを宛先に送信せずにウイルスチェックサーバ12へ自動転送する(ステップS602)。

【0037】ウイルスチェックサーバ12は電子メールサーバ24からのコネクションを受信してSPAMメールチェックを行い(ステップS603)、SPAMメールでないことが信頼できない場合にはメールセッションを破棄する(ステップS604)。SPAMメールでないことが信頼できると判断された場合には、ウイルスチェックサーバ12は電子メールを蓄積し(ステップS605)、蓄積した電子メールに対するウイルス感染チェックを行う(ステップS607)。

【0038】ウイルスチェックに必要なウイルス定義ファイルのアップデートは、アンチウイルスリサーチセンター14からのデータ更新により随時行われている(ス

テップS606)。またこのウイルスチェックにおいてはパターンマッチングの他、ミューテーション型ウイルスを発見するためのソフトマイス法、未知ウイルスの発見のためのチェックサム方式及びトラップ方式が併用されている。

【0039】ウイルスチェック(ステップS607)において異常が発見された場合、ウイルス駆除が行われる(ステップS608)。ウイルス駆除に失敗した場合、ウイルス削除が行われる(ステップS609)。ウイルス駆除またはウイルス削除により取り出されたウイルス媒体はログに書き出されて検疫される(ステップS610)。ウイルス駆除または削除が済むと、24時間体制でウイルスを常時監視するシステム運用管理統合サービスセンター16へ警告が発せられ(ステップS611)、システム運用管理統合サービスセンター16はウイルスチェックの結果ウイルスが検出されて駆除または削除された旨の報告を電子メールによりクライアントのウイルス管理者端末26に送信する(ステップS612)。報告には日時、件名、送受信メールアドレス、ウイルス名、処理結果等が含まれる。

【0040】ウイルスチェック(ステップS607)において正常と判断された電子メール及びウイルス駆除または削除済の電子メールは、DNSのMXレコードを参照して宛先の電子メールサーバへ自動転送される(ステップS613)。宛先メールサーバが受信に成功したら(ステップS614)、ウイルスチェックサーバ12からメールを削除して(ステップS615)、処理が終了する。もしも宛先メールサーバが受信に失敗した場合にはリトライが行われる。

【0041】図7はクライアント端末22が電子メールを受信するメール受信の場合の処理の流れを示す。

【0042】図7における処理は図6に示したものとほぼ同様であるが、異なる点を中心に説明する。まず、クライアントへ電子メールを送信する送信元の端末は、従来と同様にクライアントのメールアドレスを宛先にして電子メールを作成し、送信先/送信元電子メールサーバ30に対して電子メールを送信する(ステップS701)。送信先/送信元電子メールサーバ30は、予め書き換えられている宛先アドレスのDNSのMXレコードを参照し、電子メールをウイルスチェックサーバ12に自動転送する(ステップS702)。

【0043】ステップS703～S712までは図6におけるステップS603～S612における処理と同様である。

【0044】ウイルスチェック(ステップS707)において正常と判断された電子メール及びウイルス駆除(ステップS708)以下によりウイルス駆除または削除済の電子メールは、ウイルスチェックサーバ12のSMTPリレー機能を使用して、契約先の電子メールサーバへ自動転送される(ステップS713)。電子メール



\*を含むウイルスチェックシステムの主要な構成を示すブロック図であり、クライアントから電子メールを送信する場合の各部材の機能を示す。

【図2】図2は、図1と同じウイルスチェックシステムの主要な構成を示すブロック図であり、クライアント宛の電子メールを受信する場合の各部材の機能を示す。

【図3】図3は、図1と同じウイルスチェックサーバの主要な構成を示すブロック図であり、クライアントから電子メールを送信する場合の各部材の機能を示す。

【図4】図3は、図1と同じウイルスチェックサーバの主要な構成を示すブロック図であり、クライアント宛の電子メールを受信する場合の各部材の機能を示す。

【図5】図5は、図1と同じウイルスチェックサーバの各部の機能を説明する図である。

【図6】図6は、図1と同じウイルスチェックサーバのクライアントから電子メールを送信する場合の処理の流れを示すフローチャートである。

【図7】図7は、図1と同じウイルスチェックサーバのクライアント宛の電子メールを受信する場合の処理の流れを示すフローチャートである。

## 10 ウイルスチェックシステム

#### 1.4 アンチウイルスリサーチセンター

## 2.0 クライアントネットワーク

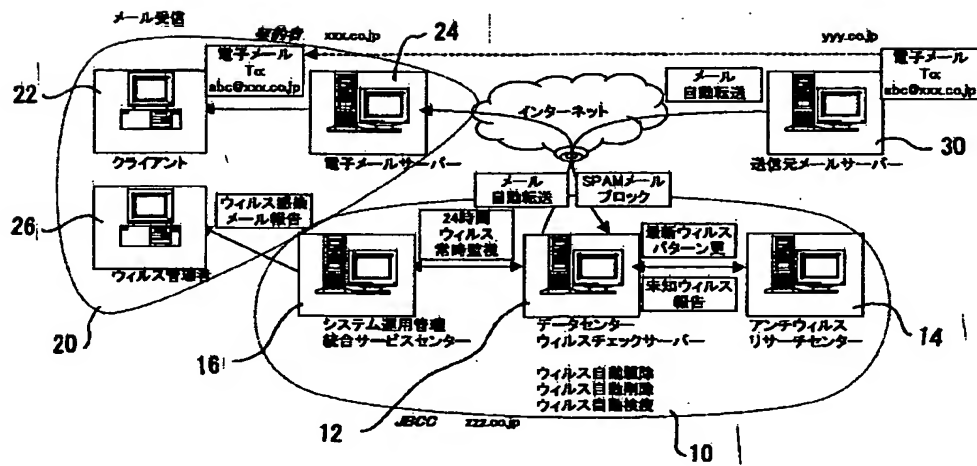
## 2.2 クライアント端末

## 24 電子メールサーバ

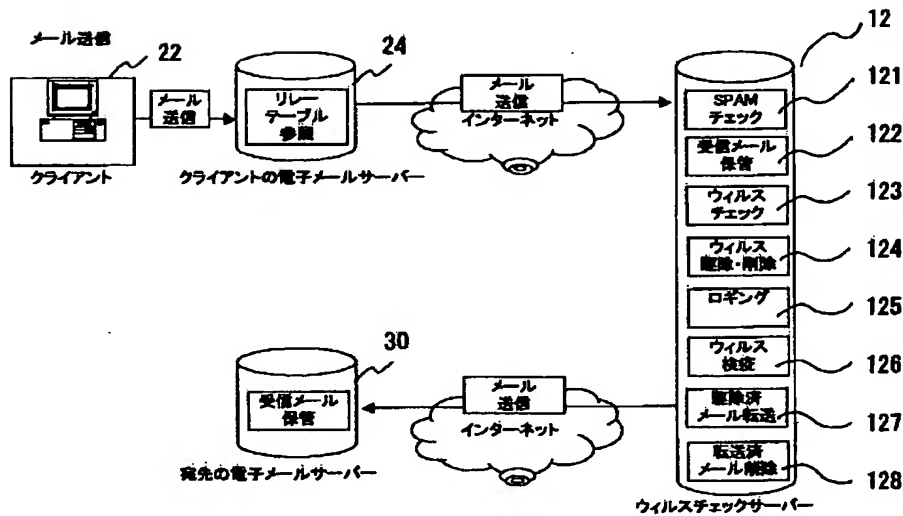
### 30 送信先/送信元電子メールサーバ

[illegible]

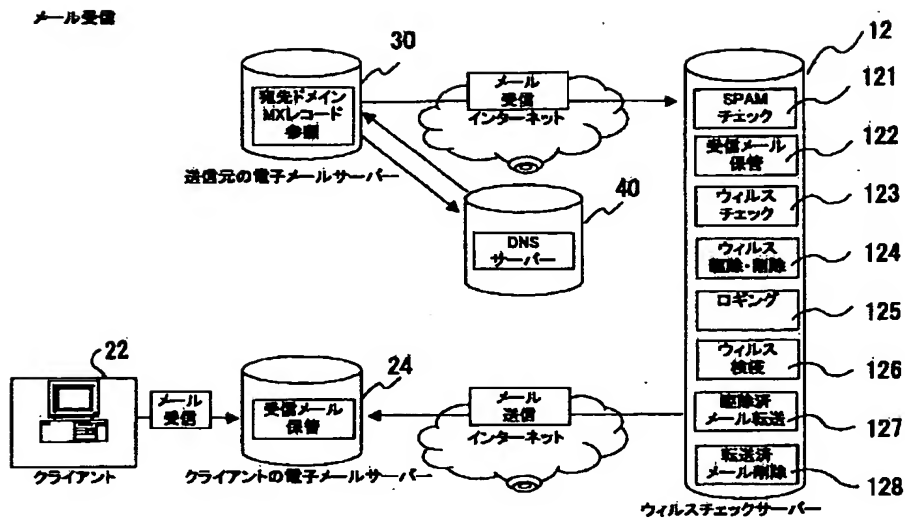
【図2】



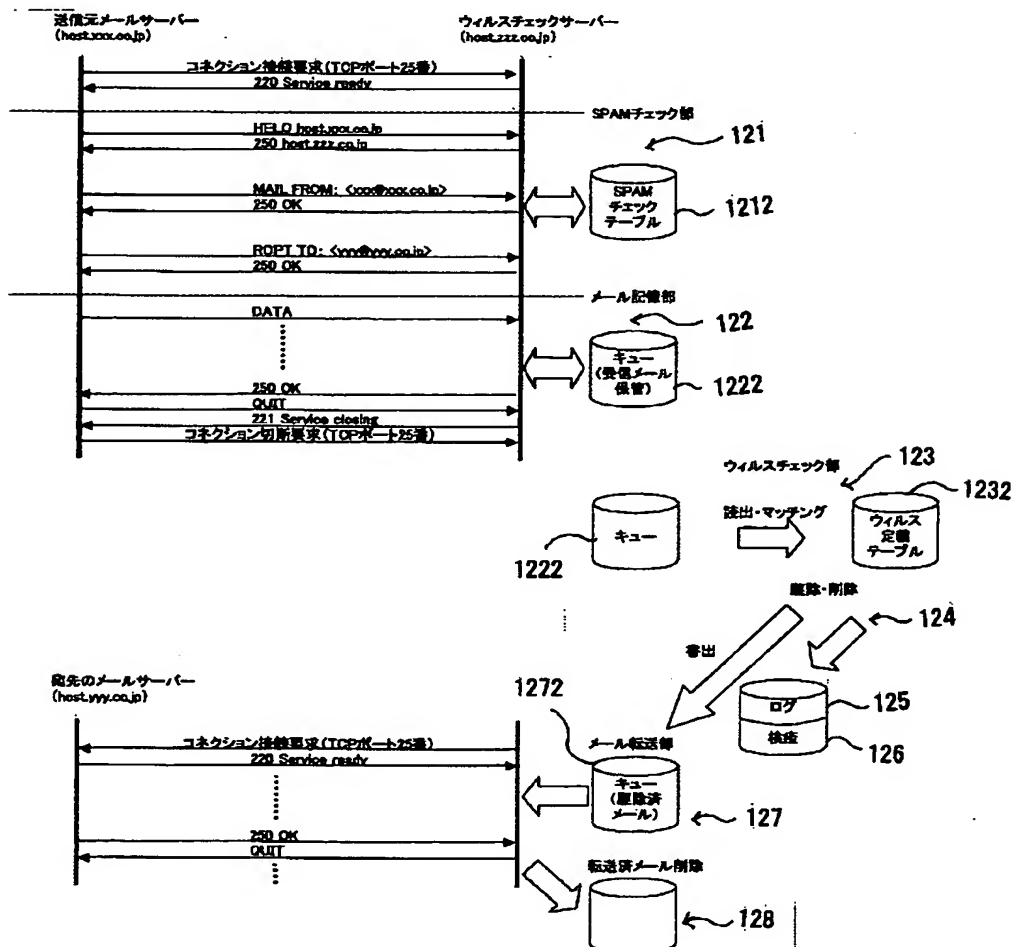
【図3】



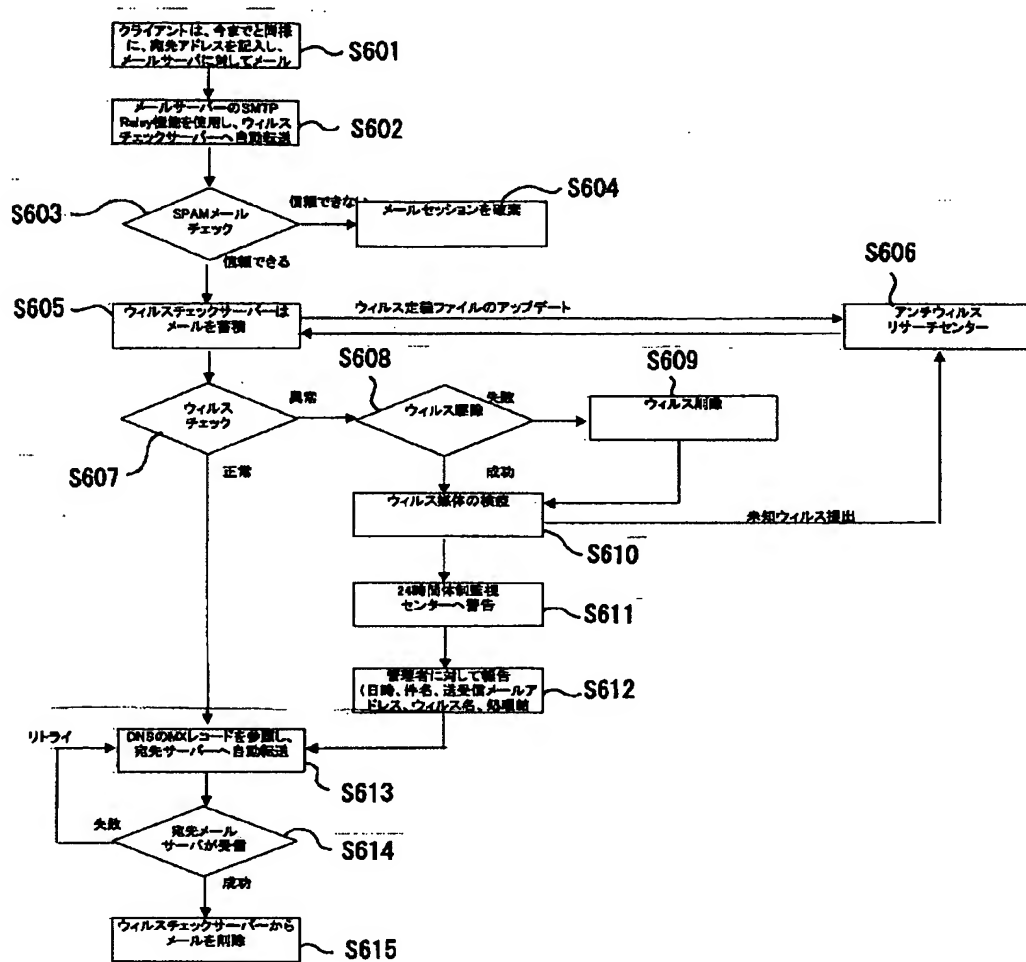
【図4】



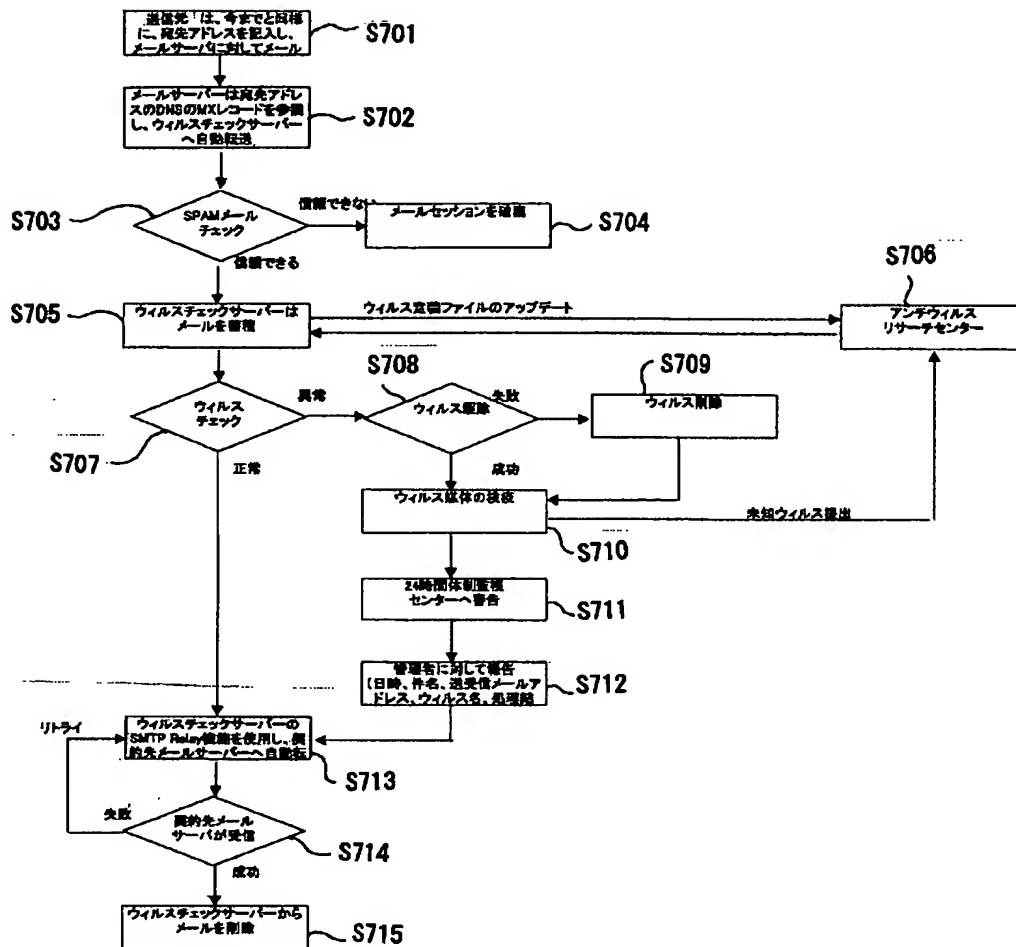
【図5】



【図6】



【図 7】



## 【手続補正書】

【提出日】平成13年11月29日（2001. 11. 29）

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

## 【特許請求の範囲】

【請求項1】一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールをインターネットを通じて受信して保管する電子メール保管手段と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック手段と、前記ウイルスチェック手段によりウイルスチェック済み

の前記電子メールを前記他の電子メールサーバにインターネットを通じて転送する電子メール転送手段とを含むことを特徴とするウイルスチェックサーバ。

【請求項2】前記一つの電子メールサーバは、クライアント側電子メールサーバであり、前記電子メール保管手段は前記クライアント側電子メールサーバから送信される前記電子メールの全てを受信して保管する請求項1に記載のウイルスチェックサーバ。

【請求項3】前記他の電子メールサーバのうちの一つはクライアント側電子メールサーバであり、前記電子メール保管手段は前記クライアント側電子メールサーバに送信される前記電子メールの全てを受信して保管する請求項1に記載のウイルスチェックサーバ。

【請求項4】前記一つの電子メールサーバ及び前記他の電子メールサーバのうちの一つは同じクライアント側電子メールサーバであり、

前記電子メール保管手段は前記クライアント側電子メールサーバに送信され、及び前記クライアント側電子メールサーバから送信される前記電子メールの全てを受信して保管する請求項 1 に記載のウイルスチェックサーバ。

【請求項 5】 前記電子メール保管手段が前記電子メールを保管する前に、前記電子メールの SPAM チェックを行う SPAM チェック手段をさらに含む請求項 1 ないし 4 に記載のウイルスチェックサーバ。

【請求項 6】 一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールをインターネットを通じて受信して電子メール保管手段に保管する電子メール保管過程と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック過程と、前記ウイルスチェック過程においてウイルスチェック済みの前記電子メールを前記他の電子メールサーバにインターネットを通じて転送する電子メール転送過程とを含むことを特徴とするウイルスチェック方法。

【請求項 7】 前記一つの電子メールサーバ及び前記他の電子メールサーバのうちの一つは同じクライアント側電子メールサーバであり、前記電子メール保管過程において、前記クライアント側電子メールサーバに送信され、及び前記クライアント側電子メールサーバから送信される前記電子メールの全てが前記電子メール保管手段に受信されて保管される請求項 6 に記載のウイルスチェック方法。

【請求項 8】 前記電子メール保管過程において、前記クライアント側電子メールサーバから送信される送信電子メールは、前記クライアント側電子メールサーバの SMTP サーバのリレー先として前記電子メール保管手段を指定することにより、前記送信電子メールの全てが前記電子メール保管手段に受信されて保管され、かつ前記クライアント側電子メールサーバに受信される受信電子メールは、DNS サーバに記述された前記クライアント側電子メールサーバについての MX レコードを前記電子メール保管手段が宛先になるように書き換えることにより、前記受信電子メールの全てが前記電子メール保管手段に受信されて保管される請求項 7 に記載のウイルスチェック方法。

【請求項 9】 前記電子メール保管過程の前に、前記電子メールの SPAM チェックを行う SPAM チェック過程をさらに含む請求項 6 ないし 8 に記載のウイルスチェック方法。

【請求項 10】 前記ウイルスチェック過程は、前記電子メール保管手段に保管された前記電子メールを読み出してウイルス定義テーブルに予め記憶された既知ウイルスとのマッチングを行うことによりウイルスに感染しているか否かを判定するウイルス感染チェック過程と、

ウイルスに感染していると判定された前記電子メールのウイルス駆除を行うウイルス駆除過程と、ウイルス駆除に失敗した場合に前記電子メールのウイルス削除を行うウイルス削除過程と、駆除または削除されたウイルス媒体の検疫を行うウイルス媒体検疫過程とを含む請求項 6 ないし 9 に記載のウイルスチェック方法。

【請求項 11】 前記ウイルス感染チェック過程においてウイルスに感染していると判定された場合に、ウイルスに感染していると判定された前記電子メールを送信した端末またはネットワークに対し報告を行う報告過程を含む請求項 10 に記載のウイルスチェック方法。

【請求項 12】 前記報告を行った前記端末またはネットワークに対し、前記端末またはネットワークからウイルスを駆除するためのウイルス駆除手段を提供し、及び／またはウイルス駆除方法を教示するウイルス駆除支援過程を含む請求項 11 に記載のウイルスチェック方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正内容】

【0005】

【課題を解決するための手段】上記目的を達成するために本発明は、一つの電子メールサーバから送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールをインターネットを通じて受信して保管する電子メール保管手段と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック手段と、前記ウイルスチェック手段によりウイルスチェック済みの前記電子メールを前記他の電子メールサーバにインターネットを通じて転送する電子メール転送手段とを含んでウイルスチェックサーバを構成した。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正内容】

【0006】本発明に係るウイルスチェックサーバにおいては、電子メールサーバからインターネットを通じて送信された電子メールは直接宛先の電子メールサーバに到着せず、いったん電子メール保管手段に保管される。電子メール保管手段に保管された電子メールは、ウイルスチェック手段により読み出されていウイルスチェックを受ける。電子メール転送手段は、ウイルスチェック手段によりウイルスチェック済みの電子メールをインターネットを通じて転送し、電子メールが宛先の電子メールサーバに到着する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】また本発明は、一つの電子メールサーバからインターネットを通じて送信された電子メールが他の電子メールサーバに到着する以前に、前記電子メールを受信して電子メール保管手段に保管する電子メール保管過程と、前記電子メール保管手段に保管された前記電子メールを読み出してウイルスチェックを行うウイルスチェック過程と、前記ウイルスチェック過程においてウイルスチェック済みの前記電子メールを前記他の電子メールサーバにインターネットを通じて転送する電子メール転送過程とを含んでウイルスチェック方法を構成した。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正内容】

【0012】本発明に係るウイルスチェック方法においては、電子メールサーバからインターネットを通じて送信された電子メールは直接宛先の電子メールサーバに到着せず、いったん電子メール保管手段に保管される。電子メール保管手段に保管された電子メールは読み出されてウイルスチェックを受け、ウイルスチェック済みの電子メールがインターネットを通じて転送され、宛先の電子メールサーバに到着する。